Written Testimony for the Oversight Hearing on "The Prevalence of Pornography, Including Child Pornography, on Peer-to-Peer Networks"

By: Randy Saaf, President of MediaDefender, Inc.

March 13th, 2003

In the summer of 2000 Napster was hitting its stride as the hottest Internet software application since the web browser. As we all know, the primary use of Napster was for the illegal trading of copyrighted music over the Internet. This was the birth of the Peer-to-Peer ("P2P") movement that continues to build momentum even today. At its peak Napster had roughly 40,000,000 users, and it could only be used for downloading audio files (MP3s). Today, P2P networks (KaZaA, Gnutella, WinMX, etc.) have roughly 80,000,000 users and are used to trade all sorts of rich media including pictures, music, pornography, television shows, movies, and software.

MediaDefender was founded in the summer of 2000 with the company calling to "Fight Crime on the Internet." In the summer of 2000 there was one primary illegal activity occurring on the P2P networks and that was the trading of copyrighted material. However, MediaDefender quickly noticed the massive quantity of pornography being traded on the Gnutella network which was much smaller than Napster but allowed trading of all media types. Napster only allowed trading of music (MP3) files, so the savvy P2P users were going to Gnutella for their porn. P2P became very efficient for downloading porn for the same reasons it was very efficient for downloading MP3s: copyright law could be avoided and big files spread quickly across the network. Amongst the large quantity of normal porn, there was an alarming quantity of legally questionable porn. We were seeing file names fly across the network that were most likely child pornography. Not surprisingly, the same feelings of guiltless anonymity that made music stealing so predominant in the P2P world were also allowing child pornography to rapidly spread. MediaDefender tried to sell our policing technology to federal law enforcement agencies like the DOJ and the FBI, but received very little interest. So, MediaDefender had to build its business solely around P2P anti-piracy, which remains its core business to this day. Since then, MediaDefender has grown to be the primary provider of P2P anti-piracy technology in the world.

Napster eventually went away, and the KaZaA network filled the void for the hungry P2P users. There have been over 197,000,000 downloads of Kazaa to date. KaZaA allows the downloading of all types of media, including picture and video files. Naturally, the largest demand and supply for video files on Kazaa is adult content. Kazaa, and most of the other P2P networks, continue to have the same alarming child pornography problem MediaDefender observed in the summer of 2000, except now the quantity is about 100,000 times larger. MediaDefender took child porn data from the KaZaA network from 3/6/03 to 3/10/03. We basically used key words that a reasonable person would associate with child porn. That data is what is being referenced for all statistics in this report. MediaDefender found 328,349 unique IPs that were running KaZaA and sharing

files that appeared to be child pornography. Presumably a unique IP is a unique computer or user excepting for dynamic IP addresses. MediaDefender found 321,153 unique movie and picture files on KaZaA that appear to be child pornography. There are roughly 4,000,000 users on KaZaA at any one time. We cannot determine the total number of people that used KaZaA over the course of our study, but it is obvious that there is a sizable child pornography presence on the network. It is also obvious that anyone can get child pornography on the network whenever they want it. I would suggest that there is probably no easier method in the word for acquiring child pornography than the P2P networks. I am concerned about the borderline pedophile that has not crossed that dangerous line yet, but it tempted to indulge his fantasy by the relative ease of the networks.

MediaDefender is primarily concerned with the child pornography problem on the P2P networks, although we realize the ease of availability of regular pornography raises an assortment of other societal issues. The fact that a 14 year old could use the same P2P network to download music and pornography is an obvious problem that I am sure will be adequately dealt with in this hearing. I want to raise the issue of that 14 year old accidentally downloading illegal child pornography to his parents' computer, and the district attorney in their county deciding to prosecute them because they are breaking a very well defined strict-liability child pornography possession law. That is a very scary scenario, but not as far fetched as it may seem. The same technology MediaDefender deploys to thwart piracy on the P2P networks can also be applied to find perpetrators of child pornography. Already, district attorneys around the nation have begun investigating cases of people sharing child pornography on P2P networks. These P2P users feel anonymous on the P2P networks, and many do not realize that the content they download is usually automatically shared up to the rest of the P2P network. Therefore, it is easy for MediaDefender to find these people. A district attorney or federal agent can give MediaDefender any school, business, or geographic region and we will probably be able to find an abundance of child pornography being shared on that IP block.

I want to make it clear that MediaDefender is never able to visually confirm the contents of the child pornography files because that, in itself, would be illegal, but the names of the files leave little doubt of their content. MediaDefender commonly finds multiple people at reputable companies and universities sharing 30 or more child pornography files apiece. MediaDefender's study found over 800 universities with computers on their networks sharing files that appeared to be child pornography. I do not know how many colleges there are in the nation, but I can assure you that almost every major college was in the list. I do not want to name names of schools and businesses at this point, but I do want to make the problem clear. Seven out of eight Ivy League schools had a combined total of over 190 computers that were serving content to the KaZaA network that appeared to be child pornography by its name and file type. Each computer probably represents a unique person at the university. It would be relatively simple for a law enforcement official to take that IP address and find the computer and student/employee it is associated with. It is also relatively simple for university officials to take that IP address and find the computer and student/employee it is associated with. I would suggest that universities and businesses start taking responsibility and proactively prevent

child pornography from being served on their networks using P2P. MediaDefender also found hundreds of very large, reputable companies serving child pornography via P2P. With a couple guesses of some of the biggest companies in America, you would probably name some of the companies I am talking about. This could be very embarrassing for these companies if it ever comes out that company resources are being used to propagate the spread of child pornography. I would additionally suggest proactive prevention by businesses before there is a widespread law enforcement effort to stop this problem. Universities and businesses cannot trust their employees to "do the right thing." Most of these students/employees are unaware that they are re-sharing the illegal child pornography they downloaded to the rest of the P2P network and that they can be easily seen by a company like MediaDefender. So, the combination of their perverseness and ignorance creates slam-dunk evidence for a policing organization to get a search warrant to walk in and seize the perpetrators hard-drive which contains the child porn. Colleges and businesses have the means to monitor the traffic on their networks and should be more responsible for illegal activity that is taking place on it.

It is unacceptable that so many of our countries most reputable universities and businesses are unwittingly dedicating their resources to the spread of child pornography. However, even more alarming is the quantity of pornography and child pornography MediaDefender finds at government institutions. Thousands of government computers are sharing pornography, including child pornography, files at many of our countries most important institutions. Heads should roll for this one because it is absolutely ridiculous that government resources are being poached for this cause. I also want to make it clear that these are not isolated slip-ups in IT. Generally, if a government organization has one computer sharing pornography on P2P, it will have at least twenty others. Of course, this also raises the very important issue of security. Many of these organizations MediaDefender found are "top secret" or defense in nature. If the people running these institutions' information technology are too inept to not realize their networks are being used to share pornography on P2P, who know what other content might be accidentally shared via P2P? One careless individual working on a top secret project accidentally sharing his entire C-drive could cause extreme havoc. If MediaDefender can monitor these government institutions for holes in their IT facilitated by P2P, so can our countries enemies. Information technology at these government organizations is clearly lacking and may be creating severe security risks for our country. Government institutions should have the knowledge and resources to prevent IT problems associated with P2P, and they should be forced to do so immediately.

There are no magic technology bullets for solving the problems associated with P2P networking. Technologies such as filters will only mildly quash the problem of P2P child pornography. The community of people sharing child pornography on the P2P networks has already devised naming codes to attempt to hide the actual content. Typically, these naming codes will be an elaborate assortment of letters and symbols that are commonly understood in the child pornography P2P community. For example, "R@ygold" is a common naming code right now. Further, there are almost a billion files on P2P at any one time. You just cannot look at what every files' content contains, and even if you could, there is a constant state of flux around what files are shared. As soon as you

identify one set of a billion files, another set of a billion files will sprout up. That is the nature of the networks. Unless a P2P network is centrally run and only allowed to distribute a closed set of content, there will never be a practical technology for preventing "illegal" content while allowing "legal" content.

The reality is that child pornography will be an ever present problem on P2P networks the same way that music piracy is an ever present problem on P2P networks. Child pornography is the highest form of unprotected speech, and law enforcement officials in both local and federal government have a duty to enforce the existing child pornography laws. P2P may seem and feel ethereal, but there are actual people at the end of every peer. Law enforcement officials must deploy technology, like MediaDefender's, to find and prosecute perpetrators of child pornography on the P2P networks.